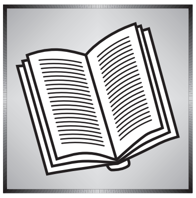

Számelmélet és valószínűségszámítás*

A matematika e két ágának összekapcsolásában úttörő szerepet játszott a 20. századi matematika két óriása, *Erdős Pál* (1913–1996) és *Turán Pál* (1910–1976), akik egymásnak is közeli barátai és munkatársai voltak. Először Erdős egyik kedvenc, részben ma is megoldatlan problémájával foglalkozunk, majd Turán egyszerű bizonyítását mutatjuk be *Geoffrey Hardy* (1877–1947) és *Srinivasa Ramanujan* (1887–1920) híres tételére az egészek prímosztóinak tipikus számáról. Mindkettő elmondható valószínűségszámítás nélkül is, de éppen a valószínűségi szemlélet mutatja meg a lényeget. Mindkét esetben a *Csebisev-egyenlőtlenséget* fogjuk alkalmazni.

1. A Csebisev-egyenlőtlenség

Egy véges *valószínűségi változó* egy olyan függvény, amely véges sok valós számértéket vesz fel, és mindegyik értéknél megmondjuk, hogy az milyen valószínűséggel adódik. Például a kockadobásnál a lehetséges értékek 1, 2, 3, 4, 5 és 6, és mindegyiknek a valószínűsége 1/6. A továbbiakban csak ilyen legegyszerűbb típusú valószínűségi változókat használunk, amelyek értékkészlete N különböző valós szám, $v_1, v_2, \ldots, v_N$, és mindegyik v_i értéket $1/N$ valószínűséggel veszi fel a változó. A valószínűségi változókat általában ξ-vel, néha η-val fogjuk jelölni.

Egy valószínűségi változó *várható értéke* a lehetséges értékeknek a valószínűségekkel súlyozott átlaga. Ezt $E(\xi)$-vel jelöljük. A mi speciális esetünkben a várható érték a felvett értékek számtani közepe:

$$E = E(\xi) = \frac{v_1 + v_2 + \ldots + v_N}{N}. \tag{1.1}$$

Pl. a kockadobás várható értéke $(1+2+3+4+5+6)/6 = 3{,}5$.

A valószínűségi változó másik fontos jellemzője a *szórás,* amit $D(\xi)$-vel jelölünk. Ezt úgy kapjuk, hogy a felvett értékeknek a várható értéktől való négyzetes eltéréseit a valószínűségekkel súlyozva átlagoljuk és az eredményből négyzetgyököt vonunk. Így a mi speciális esetünkben a négyzetes eltérések számtani közepéből kell négyzetgyököt vonni:

$$D = D(\xi) = \sqrt{\frac{(v_1 - E)^2 + \ldots + (v_N - E)^2}{N}}. \tag{1.2}$$

A szórás tehát azt méri, milyen erősen ingadozik a változó a várható érték körül. A kockadobás szórása

$$\sqrt{\frac{(1-3{,}5)^2 + (2-3{,}5)^2 + (3-3{,}5)^2 + (4-3{,}5)^2 + (5-3{,}5)^2 + (6-3{,}5)^2}{6}} \approx 1{,}71.$$

* Ehhez a témához kapcsolódik a **B. 5220.** feladat is ebben a számban.

Belátható, hogy valószínűségi változók összegének a várható értéke a várható értékek összege:

$$E(\xi+\eta)=E(\xi)+E(\eta). \tag{1.3}$$

Ha a változók *függetlenek,* akkor ugyanez érvényes a szórások *négyzetére* is:

$$D^2(\xi+\eta)=D^2(\xi)+D^2(\eta). \tag{1.4}$$

Rátérünk a két számelméleti alkalmazás valószínűségszámítási alapját képező nevezetes egyenlőtlenségre, amely *Pafnutyij Lvovics Csebisev* (1821–1894) orosz matematikustól származik. Ez informálisan azt fejezi ki, hogy egy valószínűségi változó nagy valószínűséggel a várható értékétől nem túl távoli értéket vesz fel. Itt a távolság mértékegysége a szórás.

Pontos megfogalmazásban: Jelölje a ξ valószínűségi változó várható értékét E és szórását D, továbbá legyen $c>0$ tetszőleges. Ekkor $1/c^2$-nél kisebb annak a valószínűsége, hogy a változó a várható értéktől cD-nél távolabbi értéket vesz fel:

$$P\big(|\xi-E|>cD\big)<\frac{1}{c^2}. \tag{1.5}$$

Természetesen ez csak $c>1$ esetén ad érdemi információt, hiszen a valószínűség eleve legfeljebb 1.

A speciális esetünkben ezt a következő formában fogjuk használni: Ha a változó által egyforma valószínűséggel felvett N darab v_i érték között s olyan van, amelynek a várható értéktől való eltérése nagyobb a szórás c-szeresénél, azaz s-szer fordul elő, hogy $|v_i-E|>cD$, akkor $s/N<1/c^2$.

Ennek bizonyítása:

$$ND^2=\sum_{i=1}^{N}(v_i-E)^2>\sum_{|v_i-E|>cD}(v_i-E)^2>s(cD)^2, \quad \text{így} \quad N>c^2s.$$

Az első egyenlőség az (1.2) definíció egy másik alakja, ezután az összegből csak a nagy tagokat tartottuk meg, majd ezek mindegyikét lecsökkentettük a megadott cD alsó korlátra.

2. Csupa különböző összeg

Erdős egyik kedvenc problémája: Maximálisan hány pozitív egész adható meg n-ig, hogy közülük akárhány különbözőt összeadva (beleértve az egytagú összegeket és az összes szám összegét is) mindig különböző számot kapunk? Ezt a kérdést 1931-ben vetette fel és elsőként említi híres 1993-as gólyavári előadásában, amelynek videófelvétele az interneten elérhető. Itt számos további érdekes elemi számelméleti és geometriai problémáról is beszél közérthetően, és a felvételből Erdős lenyűgöző egyéniségéről is képet kaphatunk.

A kérdést formálisan is megfogalmazzuk: Mennyi a k maximuma (n függvényében), ha az $1\leqslant a_1<a_2<\ldots<a_k\leqslant n$ egész számokból képezett minden részösszeg különböző?

Ilyen egészek például a 2 hatványai a kettes számrendszerbeli felírás egyértelműsége miatt. A 2 kitevője 0-tól $\log_2 n$ egészrészéig terjedhet, tehát

$$\max k \geqslant 1 + \lfloor \log_2 n \rfloor > \log_2 n. \tag{2.1}$$

A $\max k$ felső becsléséhez megnézzük, hány részösszeg van, és ezek milyen intervallumba eshetnek. Mivel minden részösszeg különböző egész szám, ezért legfeljebb annyi részösszeg lehet, ahány egész szám található ebben az intervallumban.

A részösszegek száma $2^k - 1$. Mindegyik legalább 1 és legfeljebb

$$n + (n-1) + \ldots + (n-k+1) \leqslant nk - 1.$$

Minden részösszeg különböző, tehát $2^k - 1$ darab egész számnak el kell férnie 1 és $nk - 1$ között. Ezért

$$2^k - 1 \leqslant nk - 1, \quad \text{azaz} \quad 2^k \leqslant nk. \tag{2.2}$$

Mindkét oldal 2-es alapú logaritmusát véve kapjuk, hogy

$$k \leqslant \log_2 n + \log_2 k. \tag{2.3}$$

Nyilván $k \leqslant n$, tehát $\log_2 k \leqslant \log_2 n$, így

$$k \leqslant 2 \log_2 n. \tag{2.4}$$

Véve (2.4)-ben mindkét oldal logaritmusát $\log_2 k \leqslant 1 + \log_2 \log_2 n$ adódik, amit (2.3)-ba beírva a

$$k \leqslant \log_2 n + \log_2 \log_2 n + 1 \tag{2.5}$$

felső becslést nyerjük.

(2.1) és (2.5) alapján

$$1 < \frac{\max k}{\log_2 n} < 1 + \frac{\log_2 \log_2 n + 1}{\log_2 n},$$

tehát

$$\lim_{n \to \infty} \frac{\max k}{\log_2 n} = 1,$$

azaz $\max k$ aszimptotikusan egyenlő $\log_2 n$-nel.

Erdős 500 dollárt ajánlott fel annak eldöntéséért, hogy $|\max k - \log_2 n|$ korlátos-e. Ez továbbra is reménytelenül nehéz.

Rátérünk a (2.1) alsó és (2.5) felső becslések javítására. Bár sokáig azt sejtették, hogy a 2-hatványok adják a legjobb konstrukciót, kiderült, hogy ennél eggyel(!) több számot is meg lehet adni, ha $n \geqslant 2^{21}$. Az továbbra is megoldatlan, hogy a kettőhatványoknál kettővel több szám megadható-e.

A felső becsléssel kapcsolatban Erdősnek és *Leo Moser* (1921–1970) kanadai matematikusnak a (2.5)-beli $\log_2 \log_2 n$-es hibatagot sikerült megfelezniük 70 évvel ezelőtt, és ma is ez a legjobb ismert eredmény. Ehhez a problémát átfogalmazták a valószínűségszámítás nyelvére. Így jött be a képbe a Csebisev-egyenlőtlenség, ami azt biztosította, hogy a részösszegek az $[1, nk-1]$ intervallumban nem egyenletesen oszlanak el, hanem az átlag közelében sűrűsödnek.

Nézzük mindezt részletesen. Legyen ξ az a valószínűségi változó, amelyik mind a 2^k darab részösszeget (beleértve az üreset is) $1/2^k$ valószínűséggel veszi fel.

Ez azt jelenti, hogy az egyes a_j egészek egymástól függetlenül 1/2–1/2 valószínűséggel szerepelnek a részösszegekben. Eszerint ξ az $\eta_1, \ldots, \eta_k$ független valószínűségi változók összege, ahol η_j a 0 és a_j értékeket veszi fel 1/2–1/2 valószínűséggel: $\xi = \sum_{j=1}^{k} \eta_j$.

Ennek megfelelően az η_j változó várható értéke és szórásnégyzete

$$E(\eta_j) = \frac{a_j}{2} \quad \text{és} \quad D^2(\eta_j) = \left(\frac{a_j}{2}\right)^2. \tag{2.6}$$

A valószínűségi változók összegének várható értékére és (függetlenség esetén) szórásnégyzetére vonatkozó (1.3) és (1.4) képletek alapján (2.6)-ból kapjuk, hogy

$$E(\xi) = \sum_{j=1}^{k} E(\eta_j) = \sum_{j=1}^{k} \frac{a_j}{2} \tag{2.7}$$

és

$$D^2(\xi) = \sum_{j=1}^{k} D^2(\eta_j) = \sum_{j=1}^{k} \left(\frac{a_j}{2}\right)^2 < \frac{kn^2}{4}. \tag{2.8}$$

1. feladat. Bizonyítsuk be (2.7)-et és (2.8)-at közvetlenül, a várható érték és szórásnégyzet additivitására történő hivatkozás nélkül. (A feladatok megoldását a cikk végén vázoljuk.)

A ξ változó szórására (2.8)-ból a $D(\xi) < n\sqrt{k}/2$ felső becslés adódik. Alkalmazzuk most az (1.5) Csebisev-egyenlőtlenséget pl. $c = 2$-vel. Ez azt jelenti, hogy az átlagtól a szórás kétszeresénél távolabb eső részösszegek száma kevesebb, mint az összes részösszeg számának a negyedrésze.

Tehát több, mint $2^k \cdot \frac{3}{4}$ összeg esik egy $4D(\xi) < 2n\sqrt{k}$ hosszúságú intervallumba, amelynek a középpontja $E(\xi)$.

Ezek az összegek mind különbözők, így

$$2^k \cdot \frac{3}{4} < 2n\sqrt{k}, \quad \text{azaz} \quad 2^k < \frac{8n\sqrt{k}}{3}. \tag{2.9}$$

Összehasonlítva (2.9)-et az első gondolatmenettel adódó (2.2)-vel, azt nyertük, hogy (2.9) jobb oldalán k helyett csak $\sqrt{k}$ egy konstansszorosa áll. Ha most a korábbihoz hasonlóan kétszer logaritmálunk, akkor ($n > 8$-ra)

$$k < \log_2 n + \frac{\log_2 \log_2 n}{2} + 2$$

adódik, tehát (2.5)-ben a hibatagot lényegében megfeleztük.

3. Tipikusan hány prímosztója van egy számnak?

Áttérünk a második számelméleti kérdésünkre. Jelölje $\omega(n)$ az n pozitív egész különböző prímosztóinak a számát. Pl. $\omega(20)=2, \omega(64)=1$. Végtelen sok n-re, a prímhatványokra $\omega(n)=1$. De bármilyen nagy is lehet: az első s prím szorzatára $\omega(n)=s$, pl.

$$\omega(2\cdot 3\cdot 5\cdot 7\cdot 11\cdot 13\cdot 17\cdot 19)=\omega(9\,699\,690)=8.$$

Bár nem nagyon látszik semmi szabályosság, belátjuk hogy egy jól ismert, „szép" $f(n)$ függvénnyel mégis teljesül, hogy a legtöbb számra $\omega(n)$ kb. $f(n)$. A „legtöbb" és „kb." kifejezések persze pontos matematikai értelmet nyernek majd.

Legyen t egy tetszőleges (nagy) pozitív egész. Először kiszámítjuk, hogy $\omega(n)$ átlagosan mekkora 1 és t között:

$$E=\frac{\omega(1)+\omega(2)+\ldots+\omega(t)}{t}=\frac{W(t)}{t}.$$

$W(t)$ becsléséhez tekintsük azt a $t\times t$-es táblázatot, amelynek az i-edik sorában az $\omega(i)$-t „számoljuk meg", azaz minden j-edik helyre 1-et írunk, ahol a j az i valamelyik prímosztója, a többi helyre pedig 0 kerül. Pl. $t=6$-ra:

	1	2	3	4	5	6
$\omega(1)=0$	0	0	0	0	0	0
$\omega(2)=1$	0	1	0	0	0	0
$\omega(3)=1$	0	0	1	0	0	0
$\omega(4)=1$	0	1	0	0	0	0
$\omega(5)=1$	0	0	0	0	1	0
$\omega(6)=2$	0	1	1	0	0	0

Tehát az i-edik sor j-edik eleme 1, ha j prímszám és osztója i-nek, egyébként pedig 0.

Hány 1-es van a táblázatban? Soronként számolva

$$\sum_{i=1}^{t}\omega(i)=W(t). \tag{3.1}$$

Most számoljunk oszloponként. Ha $j=p$ prímszám, akkor a p-edik oszlopban a p többszöröseinek megfelelő helyeken áll 1, tehát itt $\lfloor t/p\rfloor$ darab 1-es van, minden más elem 0. Így oszloponként összegezve az 1-esek száma

$$\sum_{p\leqslant t}\left\lfloor\frac{t}{p}\right\rfloor, \tag{3.2}$$

ahol az összegzés csak a prímekre történik. A továbbiakban p, q mindig prímszámot jelöl.

A soronkénti és oszloponkénti összegzést összevetve kapjuk, hogy

$$W(t)=\sum_{p\leqslant t}\left\lfloor\frac{t}{p}\right\rfloor. \tag{3.3}$$

Megjegyezzük, hogy (3.3)-at tulajdonképpen egy egyszerű összegátrendezéssel igazoltuk:

$$W(t)=\sum_{i=1}^{t}\omega(i)=\sum_{i=1}^{t}\sum_{p\mid i}1=\sum_{p\leqslant t}\sum_{p\mid i,\ i\leqslant t}1=\sum_{p\leqslant t}\left\lfloor\frac{t}{p}\right\rfloor.$$

(3.3)-at t-vel osztva adódik, hogy $\omega(n)$ átlaga $1\leqslant n\leqslant t$-re

$$E=\frac{W(t)}{t}=\frac{1}{t}\sum_{p\leqslant t}\left\lfloor\frac{t}{p}\right\rfloor=\left(\sum_{p\leqslant t}\frac{1}{p}\right)-h(t),\quad \text{ahol}\quad 0\leqslant h(t)<1. \tag{3.4}$$

Az utolsó egyenlőség az egészrészek elhagyásából adódott. Ekkor ugyanis mind a $\pi(t)$ darab tag egy 1-nél kisebb számmal nőtt, ahol $\pi(t)$ a prímek száma t-ig. Így az összeg $\pi(t)$-nél kevesebbel nőtt, ezt t-vel osztva kapjuk, hogy $0\leqslant h(t)<\pi(t)/t<1$. Mivel $\pi(t)/t$ tart a 0-hoz, ha $t\to\infty$, ennél erősebb állítás is igaz: $\lim\limits_{t\to\infty}h(t)=0$.

(3.4) tehát azt fejezi ki, hogy az 1 és t közötti egészek prímosztóinak átlagos száma lényegében a t-nél nem nagyobb prímszámok reciprokösszegével egyenlő. Felhasználjuk, hogy ez a reciprokösszeg nagyon jó közelítéssel $\ln\ln t$: létezik olyan c_1 abszolút konstans, hogy bármely t-re

$$\left|\sum_{p\leqslant t}\frac{1}{p}-\ln\ln t\right|<c_1,$$

lásd pl. [1], 5.6.2. tétel. Ez azt jelenti, hogy $\omega(n)$ átlagosan kb. $\ln\ln t$. Vagyis egy 1 és t közötti egésznek átlagosan $\ln\ln t$ különböző prímosztója van.

Az $\ln\ln x$ függvény nagyon lassan növekszik, pl. $t=10^{100}$-ra $\ln\ln t$ mindössze 5,44. Vegyük észre, hogy $\ln\ln\sqrt{t}=\ln(\ln t/2)=\ln\ln t-\ln 2$ miatt a $\sqrt{t}$ és t közötti növekedés csak $\ln 2$. Ezért az 1 és t közötti „majdnem minden" n esetén „kb. $\ln\ln t$" helyett nyugodtan mondhatunk „kb. $\ln\ln n$"-et is.

Abból azonban, hogy $\ln\ln n$ az átlag, nem következik, hogy a legtöbb esetben ehhez közeli a függvényérték, lehetnének nagy ingadozások és úgy jönne ki ez az átlag. Hardy és Ramanujan bonyolult módszerekkel belátták 1917-ben, hogy nem így van, a „legtöbb" n számnak tényleg kb. $\ln\ln n$ prímosztója van.

2. feladat. Ebben nem az a meglepő, hogy a legtöbb számnak ilyen kevés prímosztója van, hanem az, hogy ilyen sok. Magyarázzuk meg ezt a kijelentést.

3. feladat. Jelölje $\Omega(n)$ az n „összes" prímosztóinak a számát, tehát, hogy az n hány prímszám szorzata. Pl. $\Omega(20)=3$, $\Omega(64)=6$. Mutassuk meg, hogy a Hardy–Ramanujan-tétel $\Omega(n)$-re is érvényes. Ehhez igazoljuk, hogy $\sum\limits_{i=1}^{t}\big(\Omega(i)-\omega(i)\big)<t$.

A Hardy–Ramanujan-tételre Turán adott egyszerű bizonyítást 1934-ben. Ebben tulajdonképpen a Csebisev-egyenlőtlenséget használta (anélkül, hogy ennek tudatában lett volna), és ez lett a kiindulópontja a valószínűségszámítás számelméleti alkalmazásainak.

A lényeget tehát itt is a valószínűségszámítási megközelítés adja. Legyen ξ az a valószínűségi változó, amelyik az $\omega(1), \dots, \omega(t)$ értékek mindegyikét $1/t$ valószínűséggel veszi fel. Éppen ennek $E \approx \ln\ln t$ várható értékét számoltuk ki az előzőekben. Belátjuk, hogy kicsi a szórás, kisebb, mint $\sqrt{3E}$. Ekkor az (1.5) Csebisev-egyenlőtlenséget elég nagy c-vel alkalmazva ξ-nek az $E \approx \ln\ln t$ várható értéktől való eltérése 1-hez akármilyen közeli valószínűséggel $\sqrt{E}$ egy konstansszorosánál kisebb. Ez azt jelenti, hogy az 1 és t közötti majdnem minden egészre $\omega(n)$ nagyon jól közelíthető $\ln\ln t$-vel. És ahogy korábban jeleztük, majdnem minden ilyen n egészre $\ln\ln t$ helyett ez a tőle alig különböző $\ln\ln n$-nel is teljesül. Azaz valóban majdnem minden n egész számnak kb. $\ln\ln n$ különböző prímosztója van. (A precíz, formális megfogalmazást lásd pl. [1], 6.7.7. és 6.7.7a. tételek.)

Nézzük tehát a szórás felső becslését. Először Gyenes Zoltán javaslata alapján egy heurisztikus gondolatmenetet mutatunk, és utána következik majd a precíz levezetés.

A ξ változót fel tudjuk bontani prímenkénti η_p indikátorváltozók összegére. Legyen p prím és η_p értéke $1/p$ valószínűséggel 1 („a szám osztható p-vel") és $(p-1)/p$ valószínűséggel 0 („a szám nem osztható p-vel"). Ekkor

$$\xi = \sum_{p \leqslant t} \eta_p. \tag{3.5}$$

Az η_p valószínűségi változók várható értéke és szórásnégyzete

$$E(\eta_p) = \frac{1}{p} \quad \text{és} \quad D^2(\eta_p) = \frac{1}{p}\left(\frac{p-1}{p}\right)^2 + \frac{p-1}{p}\left(\frac{1}{p}\right)^2 = \frac{1}{p} - \frac{1}{p^2}. \tag{3.6}$$

Az összes pozitív egészre nézve az η_p változók függetlenek. Ugyanis a különböző prímekkel való oszthatóságok a páronként relatív prímség miatt egymástól függetlenek. Formálisan: a p-vel való oszthatóság valószínűsége $1/p$ és a $p_1, \dots, p_r$ prímek mindegyikével való oszthatóság ugyanaz, mint az $M = p_1 \cdot \ldots \cdot p_r$ szorzattal való oszthatóság, tehát ennek a valószínűsége $1/M$, ami valóban az $1/p_i$ valószínűségek szorzata.

„Kicsit" csalva tekintsük úgy, hogy az η_p változók elég nagy t-re az 1 és t közötti egészekre szorítkozva is függetlenek maradnak. Ekkor

$$D^2(\xi) = \sum_{p \leqslant t} D^2(\eta_p) = \sum_{p \leqslant t} \frac{1}{p} - \sum_{p \leqslant t} \frac{1}{p^2} \approx E.$$

A heurisztika után nézzük a precíz levezetést. Mivel $D^2(\xi) = E\big((\xi - E)^2\big) = E(\xi^2) - E^2$, itt az első tagot kell felülről becsülnünk.

$$(3.7)\qquad E(\xi^2) = \frac{1}{t}\sum_{i=1}^{t}\omega^2(i) = \frac{1}{t}\sum_{i=1}^{t}\omega(i)\sum_{p|i}1 = \frac{1}{t}\sum_{p\leqslant t}\sum_{p|i}\omega(i) =$$

$$= \frac{1}{t}\sum_{p\leqslant t}\sum_{v\leqslant t/p}\omega(vp) \leqslant \frac{1}{t}\sum_{p\leqslant t}\sum_{v\leqslant t/p}\big(1+\omega(v)\big) =$$

$$= \frac{1}{t}\sum_{p\leqslant t}\left\lfloor\frac{t}{p}\right\rfloor + \frac{1}{t}\sum_{p\leqslant t}\sum_{v\leqslant t/p}\omega(v).$$

Itt először a várható érték (1.1) definícióját alkalmaztuk ξ helyett ξ^2-re, majd az (egyik) $\omega(i)$-re beírtuk annak definícióját. Ezután átrendeztük az összeget és átírtuk a $p \mid i$ oszthatóságot $i = vp$ alakra. Az $\omega(vp) \leqslant 1 + \omega(v)$ egyenlőtlenség azért igaz, mert egy számot egy prímszámmal szorozva legfeljebb eggyel nő a prímosztók száma. Az utolsó lépésben két részre vágtuk az összeget.

(3.7) utolsó sorában az első összeg éppen $E(\xi) = E$. A második összeg belső szummáját átírjuk (3.3)-hoz hasonlóan, csak t helyett t/p-vel, majd felülről becsüljük:

$$\sum_{v\leqslant t/p}\omega(v) = \sum_{q\leqslant t/p}\left\lfloor\frac{\lfloor\frac{t}{p}\rfloor}{q}\right\rfloor < \sum_{q\leqslant t/p}\frac{t}{pq} < \frac{t}{p}\sum_{q\leqslant t}\frac{1}{q}.$$

Ennek alapján a teljes második összeg kisebb, mint

$$(3.8)\qquad \left(\sum_{p\leqslant t}\frac{1}{p}\right)^2 = \big(E + h(t)\big)^2 = E^2 + 2h(t)E + h^2(t) < E^2 + 2E.$$

(3.7) és (3.8) alapján $E(\xi^2) < E^2 + 3E$, így $D^2 = E(\xi^2) - E^2(\xi) < E^2 + 3E - E^2 = 3E$, ahogy állítottuk.

Megjegyezzük, hogy a heurisztikusan kapott eredmény is elérhető, azaz a 3-as szorzó lényegében elhagyható a szórásnégyzet felső korlátjánál. Ugyanis $\pi(t) < c_2\frac{t}{\ln t}$ alkalmas c_2 abszolút konstanssal (lásd pl. [1], 5.4.3. tétel), ezért $h(t) < \frac{\pi(t)}{t} < \frac{c_2}{\ln t}$, és így (3.8)-ban

$$2h(t)E < \frac{2c_2\cdot 1{,}01\ln\ln t}{\ln t} \to 0, \quad \text{ha}\ \ t\to\infty.$$

A feladatok vázlatos megoldása

1. Átlag: Párosítsunk minden részösszeget a komplementerével, ekkor minden ilyen pár összege $A = \sum_{j=1}^{k} a_j$. Az átlag így $2^{k-1}A/2^k = A/2$. Szórás: Egy részösszegből az $A/2$ átlagot levonva a részösszegben szereplő a_j tagok együtthatója $1/2$, a többi a_j számé pedig $-1/2$ lesz. Négyzetre emelve így mindegyik a_j^2 együtthatójára $1/4$, az a_ia_j szorzatokéra ($i < j$) pedig $\pm 1/2$ adódik. Megmutatjuk, hogy a négyzetek összeadásánál az $a_i a_j$ tagok kiesnek, mert ugyanannyiszor fordulnak elő pozitív együtthatóval, mint negatívval. Ugyanis pozitív előjelet akkor kapunk, ha a részösszegben a_i és a_j közül vagy mindkettő szerepel, vagy egyik sem. Összesen $2^{k-2}+2^{k-2}$ ilyen részösszeg van, hiszen a többi $k-2$ darab a_r mindegyike egymástól függetlenül lehet tagja vagy nem tagja a részösszegnek. Ugyanez a helyzet azokkal a részösszegekkel, amelyekben a_i és a_j közül pontosan az egyik szerepel. Így a különbségek négyzetösszegének átlaga

$$2^k \sum_{j=1}^{k} \frac{a_j^2}{4} / 2^k = \sum_{j=1}^{k} \frac{a_j^2}{4}.$$

2. Ha majdnem minden n számnak „lényegesen" több, mint $\ln\ln n$ prímosztója lenne, akkor 1 és t között ezek átlaga több lenne, mint $\ln\ln t$, ami ellentmondás. Az nyugodtan előfordulhatna, hogy a legtöbb n számnak jóval kevesebb, mint $\ln\ln n$ prímosztója van, és a nagyobb átlagot a kevés kiugró $\omega(n)$ érték okozza. Például (ellentétben az $\omega(n)$-nel és $\Omega(n)$-nel) a $d(n)$ osztók száma függvénynél ténylegesen ez a helyzet: $d(n)$ átlagértéke $\ln n$, ugyanakkor a legtöbb n egésznek csak kb. $(\ln n)^{\ln 2}$ pozitív osztója van. Ez utóbbi tény éppen a könnyen igazolható $2^{\omega(n)} \leqslant$ $\leqslant d(n) \leqslant 2^{\Omega(n)}$ kettős egyenlőtlenségből és a Hardy–Ramanujan-tételből következik.

3. A jelzett egyenlőtlenség alapján a $\Omega(n)$-re vonatkozó kérdést visszavezethetjük a $\omega(n)$-es Hardy–Ramanujan-tételre. Az egyenlőtlenség igazolásához pedig a (3.3) átalakítás mintájára lássuk be, hogy a kérdéses különbség

$$\sum_{r\geqslant 2,\ p^r\leqslant t} \left\lfloor \frac{t}{p^r} \right\rfloor .$$

Így elég megmutatni, hogy az összes (egynél nagyobb kitevőjű) prímhatvány reciprokösszege kisebb, mint 1. Egy adott p ilyen hatványainak a reciprokai mértani sorozatot alkotnak, amelynek összege $\frac{1}{p(p-1)}$. Ezeket prímek helyett minden $t \geqslant 2$ számra összegezve

$$\sum_{t=2}^{\infty} \frac{1}{t(t-1)} = \sum_{t=2}^{\infty} \left(\frac{1}{t-1} - \frac{1}{t} \right) = 1 - \frac{1}{2} + \frac{1}{2} - \frac{1}{3} + \ldots = 1.$$

Irodalom

[1] Freud Róbert–Gyarmati Edit: *Számelmélet.* Az interneten a Digitális Tankönyvtárban ingyenesen elérhető. Ebben a 12.6.3. tétel a valószínűségszámítás egy további alkalmazását is tárgyalja az Erdős és *Rényi Alfréd* (1921–1970) által bevezetett véletlen konstrukciókra támaszkodva.

Freud Róbert